UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,196	06/23/2003	Marc Solsona	042933/319264	1004

826 7590 03/20/2008

ALSTON & BIRD LLP
BANK OF AMERICA PLAZA
101 SOUTH TRYON STREET, SUITE 4000
CHARLOTTE, NC 28280-4000

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
03/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/602,196	SOLSONA ET AL.	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/12/2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on December 18, 2007.

2. Claims 1-29 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed December 18, 2007 have been fully considered but they are not persuasive.

4. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The applicant argues that on (See Page 4: second Paragraph) that "Nowhere in the cited passages does Kavsan disclose "determining integrity data for an operating system binary, wherein the integrity data enables detection of a modification to the operating system binary" as recited in Claim 1."

The examiner disagrees with the applicant's argument and analysis because "determining integrity data for an operating system binary" is an objective or goal to secure an operating system. It is not a specific technical solution. Integrity of an Operating system defines that data or codes of an operating system are not modified and makes sure that the data or codes of the

operating system are the legitimate ones. This objective or integrity of an Operating system is achieved by many techniques. One technique is to apply hash algorithm or digital signature on the data or codes of the operation system to validate the integrity of the operating system as it is well known to one f ordinary skill in the art. The other technique is to use encryption algorithm to encrypt the data or codes of the operating system with a key and the encrypted data or codes of the operating system maintains or determines integrity of the operating system under consideration. Kavsan teaches or discloses "determining integrity data for an operating system binary" by applying encryption algorithm on the data or codes of an operating system as it is also admitted or conceded by the applicant's argument (See Page 4: second Paragraph) recited as follows:

"Further, the cited passages indicate that "**encryption algorithms may be used to encrypt signals at the driver level**, such as at the Ethemet port or at the modem port, video card or disk drive, etc." **As such, Kavsan is directed to the encryption, at the kernel level, of signals and not the OS binary**. "

Furthermore the applicant's analysis is wrong when stating that encryption of the kernel level data or signal is different from OS binary. Kernel of an operating system is the core or heart of an operating system and mainly deals with the driver level devises drivers and in addition OS binary are driver level signal representations as mentioned above and also well known to one of ordinary skill in the art.

The applicant also argues in (See page 5: third paragraph) that "Reviewing the cited passages of *Teal,* these passages, and indeed all of *Teal,* are directed to methods for preventing the insertion of malicious programming code into an operating system. ***This objective is achieved in part through the modification of the operating system achieved by loading a computer code set into the kernel space that enables identification and prevention of attempts to insert unwanted computer instructions into the kernel space and/or through the kernel space into one or more user spaces***. However, *Teal* **nowhere discusses systems or methods for detecting modifications to the OS, and does not disclose modifying a kernel with integrity data**, which integrity data enables detection of a modification to the operating system binary."

Again the examiner disagrees with the applicant's argument and analysis because from the applicant's argument it appears that the applicant admits Teal discloses (see emphasis underlined) "***This objective is achieved in part through the modification of the operating system achieved by loading a computer code set into the kernel space that enables identification and prevention of attempts to insert unwanted computer instructions into the kernel space and/or through the kernel space into one or more user spaces***" and at the same time in the same argument the applicant's disagrees **without establishing any substantial distinction** (see emphasis underlined) that "*Teal* **nowhere discusses systems or methods for detecting modifications to the OS, and does not disclose modifying a kernel with integrity data**, which integrity data enables detection of a modification to the operating system binary."

The examiner would like to recite addition section from Teal to further show where "**modifying a kernel with integrity data** "as follows:

> "[0044] To authenticate the software applications running in the user space**, each set of programming instructions and associated configuration data is digitally signed, and a digital hash of each signature is retained in the kernel space**. Each time the software application is used, **the digital hash can be checked to verify that the software application is authorized to run** on the individual computer resource. **If the digital hash is not authenticated, the operating system resident in the kernel space of the individual computer resource will not allow** the software application to run in the user space." From the recited section we can see that **"modifying a kernel with integrity data**" is discloses by "each set of programming instructions and associated configuration data is digitally signed, and a digital hash of each signature is retained in the kernel space."

Therefore the applicant's argument is not persuasive to overcome the prior art Kavsan over Teal to place independent claim 1 in condition for allowance. For the same reason and analysis, the applicant's argument is not persuasive to place independent claims 8, 18, 22 and 29 in condition for allowance.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kavsan (US Pat. No.: 6,412, 069) in view of Teal et al. (hereinafter referred to as Teal, US Pub No.: 2003/0120935).

As per claim 1:

Kavsan teaches a method for protecting an operating system, comprising:

determining integrity data for an operating system binary, wherein the integrity data enables detection of a modification to the operating system binary (Column 2: lines 10-24; Column 2, lines 61-67; Column 3: lines 5-15, 20-27); and

the kernel is operable to employ the integrity data to detect the modification to the operating system binary (Column 3: lines 35-52; lines 54-65).

Kavsan does not explicitly disclose modifying a kernel with the integrity data. Teal in analogous art, however, disclose modifying a kernel with the integrity data (0035; 0044; 0067; 0091; 0095; 0097). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kavsan to include modifying a kernel with the integrity data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide owners of proprietary networks of individual computer resources to have greater security protection than is

provided by embedded security utilities, by firewall products, or by firewall products with automatic intrusion detection tools as suggested by Teal in (0032).

As per claim 2:

Teal discloses a method, wherein the integrity data further comprises at least one of a digital signature, and a hash associated with the operating system binary (0044).

As per claim 3:

Teal discloses a method, wherein the hash further comprises at least one a message digest, and a Secure Hash Algorithm (SHA) (Page 7: Paragraph 4).

As per claim 4:

Teal discloses a method, wherein the modifying the kernel further comprises:

storing the integrity data in a data store (0013; 0042; 0048; 0049; 0063; 0067); and

embedding the data store into the kernel (0013; 0042; 0048; 0049; 0063; 0067);

As per claim 5:

Teal discloses a method, wherein embedding the data store in the kernel further comprises at least one of digitally signing the data store, and encrypting the data store (0013; 0042; 0048; 0049; 0063; 0067).

7. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kavsan (US Pat. No.: 6,412, 069) in view of Teal et al. (hereinafter referred to as Teal, US Pub No.: 2003/0120935) and further in view of Pham et al. (US Pub No.: 2004/0078568).

As per claim 6:

Teal teaches generating an operating system image based in part on the modified kernel and the operating system user level binary (0094-0095).

Kavsan and Teal do not explicitly disclose the operating system image comprises at least one of creating an archive file, a compressed file, and a Cabinet (CAB) file. Pham et al. in analogous art, however, disclose the operating system image comprises at least one of creating an archive file, a compressed file, and a Cabinet (CAB) file (Figure 5B: 42; Figure 12: 388). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kavsan and Teal to include the operating system image comprises at least one of creating an archive file, a compressed file, and a Cabinet (CAB) file. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an efficient mechanism for reliably securing persistent data in a manner eminently subject to cooperative management and control within a security domain as suggested by Pham et al. in (Page 2: 0012).

As per claim 7:

Kavsan discloses a method, wherein the operating system binary further comprises at least one of an OS user level binary, and the kernel (Figure 1: Application Space; Kernel Space).

8. Claims 8-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eun et al. (WO 01/80482 A1) in view of Teal et al. (hereinafter referred to as Teal, US Pub No.: 2003/0120935).

As per claim 8:

Eun et al. disclose a method for protecting an operating system, comprising;

generating a first integrity data for an operating system binary (Page 5: lines 11-20; lines 28-34; Page 6: lines 4-11);

receiving a request associated with the operating system binary (Page 8: lines 15-22);

retrieving the first integrity data associated with the operating system binary (Figure 3: 312, 314 318);

determining if the first integrity data indicates tampering of the operating system binary (Figure 3: 310 308 306); and

performing a tamper detection action if the first integrity data indicates tampering of the operating system binary (Figure 3: 310 308 306).

Eun et al. do not explicitly disclose modifying an operating system kernel with the first integrity data. Teal in analogous art, however, disclose modifying an operating system kernel with the first integrity data (0035; 0044; 0067; 0091; 0095; 0097). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Eun et al. to include modifying an operating system kernel with the first integrity data. This modification would have been obvious because a person having ordinary skill

in the art would have been motivated to do so to provide owners of proprietary networks of individual computer resources to have greater security protection than is provided by embedded security utilities, by firewall products, or by firewall products with automatic intrusion detection tools as suggested by Teal in (0032).

As per claim 9:

Eun et al. disclose a method, wherein receiving the request further comprises receiving at least one of a read action, an execute operation, and an install request (Figure 8: 702).

As per claim 10:

Teal discloses a method, wherein performing the tamper detection action further comprises at least one of providing a tamper detection message, and quarantining the operating system binary (0021; 0041; 0042; 0074; 0079).

As per claim 11:

Teal discloses a method, wherein the first integrity data further comprises at least one of a digital signature, and a hash associated with the operating system binary (0013; 0042; 0048; 0049; 0063; 0067).

As per claim 12:

Teal discloses a method, wherein the hash further comprises at least one a message digest, and a Secure Hash Algorithm (SHA) (0013; 0042; 0048; 0049; 0063; 0067).

As per claim 13:

Teal discloses a method, wherein modifying the operating system kernel with the first integrity data further comprises storing the first integrity data in at least one of a database, a file, and a program (0013; 0042; 0048; 0049; 0063; 0067).

As per claim 14:

Teal discloses a method, wherein modifying the operating system kernel further comprises associating the first integrity data with the operating system kernel (0013; 0042; 0048; 0049; 0063; 0067).

As per claim 15:

Teal discloses a method, wherein associating the first integrity data with the operating system kernel further comprises digitally signing the first integrity data with a digital key associated with the operating system kernel (0013; 0042; 0048; 0049; 0063; 0067).

As per claim 16:

Eun et al. disclose a method, wherein determining if the first integrity data indicates tampering of the operating system binary further comprises:

determining a second integrity data for the operating system binary (Page 2: lines 15-27; Abstract; Page 7: lines 15-20);

determining if the first integrity data is substantially different from the second integrity data (Page 6: lines 25-36); Page 7: lines 15-20); and

indicating tampering of the operating system binary if the first integrity data is substantially different from the second integrity data (Page 13: lines 16-33).

As per claim 17:

Eun et al. disclose a method, wherein determining if the first integrity data is substantially different from the second integrity data further comprises comparing the second integrity data to the first integrity data (Page 2: lines 15-27; Abstract; Page 7: lines 15-20).

As per claim 18:

Eun et al. disclose a method for protecting an operating system, comprising:

receiving a request associated with an operating system binary (Page 8: lines 15-22);

retrieving integrity data associated with the operating system binary (Figure 3: 312, 314 318); and

performing a tamper detection action if the integrity data indicates tampering of the operating system binary (Figure 3: 310 308 306).

Eun et al. do not explicitly disclose modifying an operating system kernel. Teal in analogous art, however, disclose modifying an operating system kernel (0035; 0044; 0067; 0091; 0095; 0097). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Eun et al. to include

modifying an operating system kernel. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide owners of proprietary networks of individual computer resources to have greater security protection than is provided by embedded security utilities, by firewall products, or by firewall products with automatic intrusion detection tools as suggested by Teal in (0032).

As per claim 19:

Eun et al. disclose a method, wherein receiving the request further comprises receiving at least one of a read action, an execute operation, and an install request (Figure 8: 702).

As per claim 20:

Teal discloses a method, wherein performing the tamper detection action further comprises at least one of providing a tamper detection message, and quarantining the operating system binary (0021; 0041; 0042; 0074; 0079).

As per claim 21:

Eun et al. disclose a method, wherein determining if the integrity data indicates tampering of the operating system binary further comprises:

determining another integrity data for the operating system binary (Page 2: lines 15-27; Abstract; Page 7: lines 15-20);

determining if the other integrity data is substantially different from the retrieved integrity data (Page 6: lines 25-36); Page 7: lines 15-20); and

indicating tampering of the operating system binary if the other integrity data is substantially different from the retrieved integrity data (Page 13: lines 16-33).

As per claim 22:

Eun et al. disclose a computer-readable medium having computer-executable components for protecting an operating system, comprising:

a data store configured to receive and store a first integrity data, wherein the first integrity data is for an operating system binary (Figure 3: 312, 314, 316, 318); and

receiving a request to examine an operating system binary (Page 6: lines 5-11; Page 7: 4-22);

retrieving the first integrity data for the operating system binary (Page 8: lines 11-22);

determining if the first integrity data indicates tampering of the operating system binary (Page 11: lines 15-33).

Eun et al. do not explicitly disclose a tamper detection component, coupled to the data store, that is arranged to perform actions, and performing a tamper detection action if the first integrity data indicates tampering of the operating system binary. Teal in analogous art, however, disclose a tamper detection component, coupled to the data store, that is arranged to perform actions, and performing a tamper detection action if the first integrity data indicates tampering of the operating system binary (0037, 0041; 0044; 0067; 0091; 0095; 0097). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Eun et al. to include a tamper detection component, coupled to

the data store, that is arranged to perform actions, and performing a tamper detection action if the first integrity data indicates tampering of the operating system binary.. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide owners of proprietary networks of individual computer resources to have greater security protection than is provided by embedded security utilities, by firewall products, or by firewall products with automatic intrusion detection tools as suggested by Teal in (0032).

As per claim 23:

Teal discloses a computer-readable medium, wherein the computer-executable components are associated with an operating system kernel (0037, 0041; 0044; 0067; 0091; 0095; 0097).

As per claim 24:

Teal discloses a computer-readable medium, wherein performing the tamper detection action further comprises at least one of providing a tamper detection message, and quarantining the operating system binary (0021; 0041; 0042; 0074; 0079).

As per claim 25:

Eun et al. disclose a computer-readable medium, wherein the first integrity data further comprises at least one of a digital signature, and a hash associated with the operating system binary (Figure 3: 304).

As per claim 26:

Eun et al. disclose a computer-readable medium, wherein the operating system binary further comprises at least one of an OS user level binary, and a kernel (Figure 2: User Level, Kernel Level).

As per claim 27:

Pham et al. discloses a computer-readable medium, wherein determining if the first integrity data indicates tampering of the operating system binary further comprises:

determining a second integrity data for the operating system binary (Figure 5B: 156);

determining if the first integrity data is substantially different from the second integrity data (Figure 10B: 298), and

indicating tampering of the operating system binary if the first integrity data is substantially different from the second integrity data (Figure 10B: lines 302).

As per claim 28:

Eun et al. a computer-readable medium, wherein the second integrity data further comprises at least one of a digital signature, and a hash associated with the operating system binary (Figure 3: 304).

As per claim 29:

Eun et al. disclose an apparatus for protecting an operating system, comprising: means for receiving a request to examine an operating system binary;

means for retrieving a first integrity data for the operating system binary (Page 8: lines 11-22);

means for determining a second integrity data for the operating system binary (Page 6: lines 25-36); Page 7: lines 15-20); and

Eun et al. do not explicitly disclose means for determining if the first integrity data is substantially different from the second integrity data, and if the first integrity data is substantially different from the second integrity data, a means for performing a tamper detection action. Teal in analogous art, however, disclose means for determining if the first integrity data is substantially different from the second integrity data, and if the first integrity data is substantially different from the second integrity data, a means for performing a tamper detection action (0037, 0041; 0044; 0067; 0091; 0095; 0097). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Eun et al. to include means for determining if the first integrity data is substantially different from the second integrity data, and if the first integrity data is substantially different from the second integrity data, a means for performing a tamper detection action. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide owners of proprietary networks of individual computer resources to have greater security protection than is provided by embedded security utilities, by firewall products, or by firewall products with automatic intrusion detection tools as suggested by Teal in (0032).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137